日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年　６月２１日

出 願 番 号
Application Number: 平成１１年特許願第１７４０６６号

出 願 人
Applicant (s): 株式会社日立製作所

２０００年　２月１８日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

出証番号　出証特２０００－３００７５５１

【書類名】　特許願

【整理番号】　PNT990345

【提出日】　平成11年 6月21日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 19/00

【発明者】

【住所又は居所】　東京都江東区新砂一丁目６番２７号　株式会社日立製作所　公共情報事業部内

【氏名】　三浦　淳一

【発明者】

【住所又は居所】　東京都江東区新砂一丁目６番２７号　株式会社日立製作所　公共情報事業部内

【氏名】　斎藤　由紀夫

【発明者】

【住所又は居所】　東京都江東区新砂一丁目６番２７号　株式会社日立製作所　公共情報事業部内

【氏名】　小磯　良太

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社日立製作所

【代理人】

【識別番号】　100061893

【弁理士】

【氏名又は名称】　高橋　明夫

【電話番号】　03-3661-0071

【選任した代理人】

【識別番号】　100086656

【弁理士】

【氏名又は名称】　田中　恭助

【電話番号】　03-3661-0071

【手数料の表示】

【予納台帳番号】　011626

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　電子認証方法及びプログラム格納媒体

【特許請求の範囲】

【請求項１】

サービスを要求する側の第１の計算機とサービスを提供する側の第２の計算機とがネットワークを介して接続され、第２の計算機から第１の計算機へ要求されたコンテンツを送信し、該コンテンツに関して第１の計算機から第２の計算機へデータを送信するシステムの電子認証方法において、

第２の計算機によって該コンテンツのアクセス対応にアクセス番号を生成して記憶装置に登録するとともに該コンテンツ内に該アクセス番号を視覚不可なように埋め込んで第１の計算機へ送信し、第１の計算機によって該コンテンツを表示し、該コンテンツに関して入力されたデータに該コンテンツから取り出した該アクセス番号を付加して第２の計算機へ送信し、第２の計算機によつて受信した該アクセス番号が登録済であるときに受信したデータの正当性を認証するとともに登録された該アクセス番号を無効にすることを特徴とする電子認証方法。

【請求項２】

第２の計算機は、さらに該コンテンツのアクセス対応に公開鍵と秘密鍵を生成して記憶装置に登録するとともに該コンテンツ内に該公開鍵を視覚不可なように埋め込んで第１の計算機へ送信し、第１の計算機によって該コンテンツに関して入力されたデータを該コンテンツから取り出した該公開鍵によって暗号化して第２の計算機へ送信し、第２の計算機によって受信した該アクセス番号が登録済であるときに登録された該秘密鍵によって受信したデータを復号することを特徴とする請求項１記載の電子認証方法。

【請求項３】

計算機読み取り可能なプログラムを格納する記憶媒体であって、該プログラムは、外部から要求されたコンテンツのアクセス対応にアクセス番号を生成する機能と、生成されたアクセス番号を記憶装置に登録する機能と、該コンテンツ内に該アクセス番号を視覚不可なように埋め込んで外部へ送信する機能と、外部から該アクセス番号を付加したデータを受信する機能と、受信した該アクセス番号が

登録済であるときに受信したデータの正当性を認証するとともに、登録された該アクセス番号を無効にする機能とを有することを特徴とするプログラムの記憶媒体。

【請求項４】

前記プログラムは、さらに該コンテンツのアクセス対応に公開鍵と秘密鍵を生成する機能と、生成された公開鍵と秘密鍵を記憶装置に登録する機能と、該コンテンツ内に該公開鍵を視覚不可なように埋め込んで外部へ送信し、外部から該公開鍵によつて暗号化された該データを受信する機能と、受信した該アクセス番号が登録済であるときに登録された該秘密鍵によって受信したデータを復号する機能とを有することを特徴とする請求項３記載のプログラムの記憶媒体。

【請求項５】

計算機読み取り可能なプログラムを格納する記憶媒体であって、該プログラムは、外部から受信したコンテンツを表示する機能と、該コンテンツに関してデータ入力を受ける機能と、該コンテンツ内に視覚不可なように埋め込まれたアクセス番号を取り出す機能と、入力された該データに該アクセス番号を付加して外部へ送信する機能とを有することを特徴とするプログラムの記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、サービスを提供する側の計算機からサービスを要求する側の計算機へコンテンツを送信し、このコンテンツに関して後者の計算機から前者の計算機へ入力データを送信するシステムに係わり、特に正当なコンテンツアクセスに関する入力データであることを認証する電子認証方法に関する。

【０００２】

【従来の技術】

インターネットを利用する電子商取引の分野では、本人認証、データの改ざん防止等のセキュリティ技術が重要である。従来のセキュリティ技術としてパスワード方式、データを暗号化するための種々の暗号化方式、電子証明書発行など様々な努力が払われてきた。例えばインターネット上でクレジットカード決済を安

全に行うプロトコル仕様であるＳＥＴ（Ｓｅｃｕｒｅ　Ｅｌｅｃｔｒｏｎｉｃ　Ｔｒａｎｓａｃｔｉｏｎｓ）、ベリサイン社の電子認証システムなどを挙げることができる。

【０００３】

【発明が解決しようとする課題】

インターネットを利用するシステムでは、一般にクライアントがWWW（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）サーバにコンテンツを要求し、WWWサーバがクライアントへ要求されたコンテンツを送信し、クライアントが受信したコンテンツを表示装置上に表示する。クライアントがこのコンテンツに関してデータを入力し、入力されたデータをWWWサーバへ送信すると、WWWサーバが受信したデータの処理を実行する。ここでクライアント側でコンテンツのコピーが容易であるため、コンテンツのコピーを採取しておいて再利用し、許可されていないデータをWWWサーバへ送信したり、他人がコンテンツ画面を介して入力したデータを改ざんしてWWWサーバへ送信するといった不正が発生する可能性がある。

【０００４】

本発明の目的は、提供されるコンテンツに対して応答されるデータが正当なコンテンツアクセスに関する入力データであることを認証する方法を提供することにある。

【０００５】

また本発明の他の目的は、このような電子認証方法を実現するためのプログラムを格納する記憶媒体を提供することにある。

【０００６】

【課題を解決するための手段】

本発明は、サービスを要求する側の第１の計算機とサービスを提供する側の第２の計算機とがネットワークを介して接続され、第２の計算機から第１の計算機へ要求されたコンテンツを送信し、該コンテンツに関して第１の計算機から第２の計算機へデータを送信するシステムの電子認証方法において、第２の計算機によってコンテンツのアクセス対応にアクセス番号を生成して記憶装置に登録するとともにこのコンテンツ内にそのアクセス番号を視覚不可なように埋め込んで第

１の計算機へ送信し、第１の計算機によってこのコンテンツを表示し、このコンテンツに関して入力されたデータにコンテンツから取り出したアクセス番号を付加して第２の計算機へ送信し、第２の計算機によつて受信したそのアクセス番号が登録済であるときに受信したデータの正当性を認証するとともに登録されたアクセス番号を無効にする電子認証方法を特徴とする。

【０００７】

また本発明は、上記方法を第１の計算機で実行されるプログラム又は第２の計算機で実行されるプログラムとして格納する記憶媒体を特徴とする。

【０００８】

【発明の実施の形態】

以下、本発明の一実施形態について図面を用いて説明する。

【０００９】

図１は、本実施形態のインターネットを利用してサービスを提供するシステムの構成図である。システムはクライアント１、ＷＷＷサーバ２及び両者を接続するネットワークであるインターネット３から構成される。クライアント１は、サービス要求を発行しサービスを受ける側のパソコンなどの計算機であり、その処理装置には、表示装置１１及び入力装置１２が接続される。またそのメモリにはＷＷＷブラウザ１３が格納され、処理装置によって実行される。表示装置１１はコンテンツの内容を表示する装置、入力装置１２はデータ及び指令を入力する装置である。ＷＷＷブラウザ１３は、インターネット３を介してＷＷＷサーバ２へコンテンツを要求し、得られたコンテンツを表示装置１１に表示する。また入力装置１２を介して入力されたデータをＷＷＷサーバ２へ送信する。

【００１０】

ＷＷＷサーバ２は、サービスを提供する側の計算機であり、その処理装置に接続される記憶装置上にアクセス管理テーブル２１及びコンテンツＤＢ（データベース）２２を格納する。アクセス管理テーブル２１は、コンテンツへのアクセスを管理するための認証情報を格納する。コンテンツＤＢ２２は、クライアント１に提供するコンテンツを格納するＤＢである。ここでコンテンツとは、ＷＷＷサーバ２に蓄積されクライアント１に提供される表示画面情報であり、テキストデ

ータ、イメージデータ、静止画、動画などのうち少なくとも１つを含む情報である。WWWサーバ２のメモリに格納されその処理装置で実行されるWWWサーバプログラム２３は、クライアント１の要求に従ってクライアント１へコンテンツを送信するとともに、各コンテンツ要求ごとにアクセス管理テーブル２１に認証情報を格納し、そのコンテンツに係わるクライアント１から送られるデータの認証を行う。

【００１１】

なお本発明の電子認証機能を含むWWWサーバプログラム２３を記憶媒体に格納して、WWWサーバ２の駆動装置を介してWWWサーバ２のメモリに読み込むか、ネットワークを介する伝送によってWWWサーバ２へ伝送し、WWWサーバ２のメモリに格納してWWWサーバ２の処理装置によつて実行することが可能である。本発明の電子認証機能を含むWWWブラウザ１３についても同様に、そのプログラムを記憶媒体に格納して、クライアント１の駆動装置を介してクライアント１のメモリに読み込むか、ネットワークを介する伝送によってクライアント１へ伝送し、クライアント１のメモリに格納してクライアント１の処理装置によつて実行することが可能である。

【００１２】

図２は、アクセス管理テーブル２１を構成する各アクセス情報レコードのデータ形式を示す図である。同レコードは、アクセス番号４１、公開鍵４２、秘密鍵４３および登録日時４４の各項目から構成される。アクセス番号４１はコンテンツにアクセスするごとに生成され、そのコンテンツアクセスに付随する番号である。公開鍵４２はそのコンテンツに関してクライアント１から送信されるデータの機密を保護するために生成される暗号鍵である。秘密鍵４３は公開鍵４２によって暗号化された暗号文を復号するための復号鍵である。アクセス番号４１、公開鍵４２及び秘密鍵４３は、コンテンツアクセスごとに生成される。登録日時４４は当該アクセス情報レコードが登録された日時（日付，時刻）である。

【００１３】

図３Ａ及び図３Ｂは、クライアント１のWWWブラウザ１３及びWWWサーバ２のWWWサーバプログラム２３の処理の流れを示すフローチャートである。W

ＷＷブラウザ１３がＷＷＷサーバ２へコンテンツ要求を送信すると（ステップ５１）、ＷＷＷサーバプログラム２３はこのコンテンツ要求を受信する（ステップ５２）。次に乱数を発生させてアクセス番号を採番し（ステップ５３）、また公開鍵暗号方式に従って公開鍵及びその秘密鍵を生成する（ステップ５４）。次にコンテンツＤＢ２２を検索して要求されたコンテンツを取り出し（ステップ５５）、電子透かしの技術を用いてそのコンテンツに生成したアクセス番号と公開鍵をユーザによって視覚できないように埋め込む（ステップ５６）。これらの情報を埋め込むコンテンツ上の位置としては、位置決めの便のためにインターネットマーク、ロゴマークなど特定のマークを包含する矩形領域が望ましい。また電子透かしの技術の適用の容易性からみて濃淡画像領域が望ましい。次に生成したアクセス番号４１、公開鍵４２及び秘密鍵４３に登録日時４４を加えて新しいアクセス情報レコードとしてアクセス管理テーブル２１に登録する（ステップ５７）。次にこのようにして認証情報を埋め込んだコンテンツをクライアント１へ送信する（ステップ５８）。

【００１４】

ＷＷＷブラウザ１３は、このコンテンツを受信し（ステップ５９）、表示装置１１上に表示する（ステップ６０）。ここでコンテンツはユーザが視覚できるように表示されるが、埋め込まれたアクセス番号と公開鍵は表示されず、ユーザは視覚によって認識できない。入力装置１２を介してデータが入力されたとき（ステップ６１）、図３Ｂに移り、ＷＷＷブラウザ１３は、コンテンツから電子透かしが埋め込まれている位置を取得し、埋め込まれたアクセス番号と公開鍵を取り出す（ステップ６２）。次に入力されたデータをこの公開鍵によって暗号化して電文を作成し（ステップ６３）、この電文にアクセス番号を付加してＷＷＷサーバ２へ送信する（ステップ６４）。アクセス番号を暗号化してもよいが、秘密性が少ないので特に暗号化する必要はない。

【００１５】

ＷＷＷサーバプログラム２３はこの電文を受信し（ステップ６５）、受信したアクセス番号によってアクセス管理テーブル２１を検索する（ステップ６６）。該当するアクセス情報レコードが存在すれば（ステップ６７ＹＥＳ）、電文の暗

号化されている部分を秘密鍵によって復号化する（ステップ６８）。該当するアクセス情報レコードが存在しなければ（ステップ６７ＮＯ）、受信した電文を破棄する（ステップ６９）。次に復号化されたデータがあらかじめ予想される意味のあるデータか否かによつて復号化できたか否かを判定する（ステップ７０）。復号化できた場合（ステップ７０ＹＥＳ）には、当該アクセス情報レコードをアクセス管理テーブル２１から削除し（ステップ７１）、受信したデータに基づいて以降の処理を実行する（ステップ７２）。復号化できない場合（ステップ７０ＮＯ）には、受信した電文を破棄し（ステップ７３）、当該アクセス情報レコードをアクセス管理テーブル２１から削除する（ステップ７４）。以降の処理は行わない。アクセス情報レコードの削除は、一般的にはそのレコードを無効にするということになる。

【００１６】

なおWWWサーバ２は、周期的にアクセス管理テーブル２１に登録されたアクセス情報レコードの登録日時４４をチェックし、所定時間以上経過したアクセス情報レコードをアクセス管理テーブル２１から削除する。これによってデータ入力による応答のないコンテンツアクセスの認証を中止する。

【００１７】

上記実施形態によれば、クライアント１へ送られるコンテンツにはアクセス番号が埋め込まれ、このアクセス番号はコンテンツアクセスごとに生成されるので、このコンテンツをコピーしてデータ入力し、WWWサーバ２へ送信してもすでにそのアクセス番号はWWWサーバ２によって無効化されていることになり、WWWサーバ２へ送信されるデータは無効となる。またクライアント１からインターネット３を介してWWWサーバ２へ電文を送信する途中でアクセス番号が盗聴されたとしてもそのアクセス番号を再利用しようとすると無効となる。クライアント１のユーザがコンテンツに埋め込まれているアクセス番号を解読しても同様であり、他の目的のために再利用できない。

【００１８】

また上記実施形態によれば、クライアント１へ送られるコンテンツには１回使用に限定される公開鍵が埋め込まれているので、クライアント１からWWWサー

バ２へ送られる個人情報など秘密性のある情報を保護することができる。この公開鍵によって暗号化された情報が盗聴されたとしても再利用できず、従って他人の個人情報を盗聴して本人になりすましたり、他人の注文書の金額、数量などを改ざんするなどの不正を防止できる。

【００１９】

上記実施形態では電子透かしの技術を利用するが、その主たる目的は、アクセス番号及び公開鍵はコンテンツの内容ではなくユーザに知らせる必要がないので電子透かしの方法を用いて隠しておくことにあり、特に電子透かしの方法に秘密性があるわけではない。従って電子透かしの方式は、多くのコンテンツに広く適用でき、WWWブラウザ１３及びWWWサーバプログラム２３に共通に適用できるように単純で確実に電子透かしを埋め込める方式が望ましい。

【００２０】

また上記実施形態では、WWWサーバ２は乱数発生によつてアクセス番号を生成したが、コンテンツの著作権保護など他の目的にも利用するためにアクセス番号の生成を連番（通し番号）としてもよい。ただしアクセス番号を連番とすると、コンテンツ中のアクセス番号の解読によって将来のコンテンツアクセスの際に生成されるアクセス番号が予想される危険性がある。またアクセス番号の桁数を多くとり、ハッシュ関数によつてハッシュ値を求め、コンテンツ中にアクセス番号のハッシュ値を埋め込んでもよい。その場合にはアクセス番号４１にはハッシュ値を格納し、ステップ６６ではハッシュ値によってアクセス管理テーブル２１を検索することになる。

【００２１】

本発明により、インターネットを利用する電子商取引、インターネット・ショッピングなどにおいてWWWサーバ２からクライアント１へ送られたコンテンツに関してクライアント１からWWWサーバ２へ個人情報、取引データなどを送信する際にその個人情報、取引データなどが正当なコンテンツアクセスに関する入力データであることを証明できる。またユーザのミスによって１つの注文書に対して２つ以上の注文を発行するなど二重に取引データを送信するミスも防止できる。

【００２２】

【発明の効果】

以上述べたように本発明によれば、サーバがクライアントに提供するコンテンツにはアクセス番号が付随し、このコンテンツに関するサーバへの応答データにはアクセス番号が伴うため、１回のコンテンツアクセスに関する応答データは１回のみに限定することができ、コンテンツのコピーを利用する許可されていない応答データやデータの改ざんを目的とした不正な応答データを排除し、入力データが正当なコンテンツアクセスに関する応答データであることを認証できる。また応答データを１回限りの公開鍵によって暗号化することができ、応答データの盗聴を防止することができる。

【図面の簡単な説明】

【図１】

実施形態のインターネットを利用してサービスを提供するシステムの構成図である。

【図２】

実施形態のアクセス管理テーブル２１のデータ構成を示す図である。

【図３Ａ】

実施形態のシステムの処理の流れを示すフローチャートである。

【図３Ｂ】

実施形態のシステムの処理の流れを示すフローチャート（続き）である。

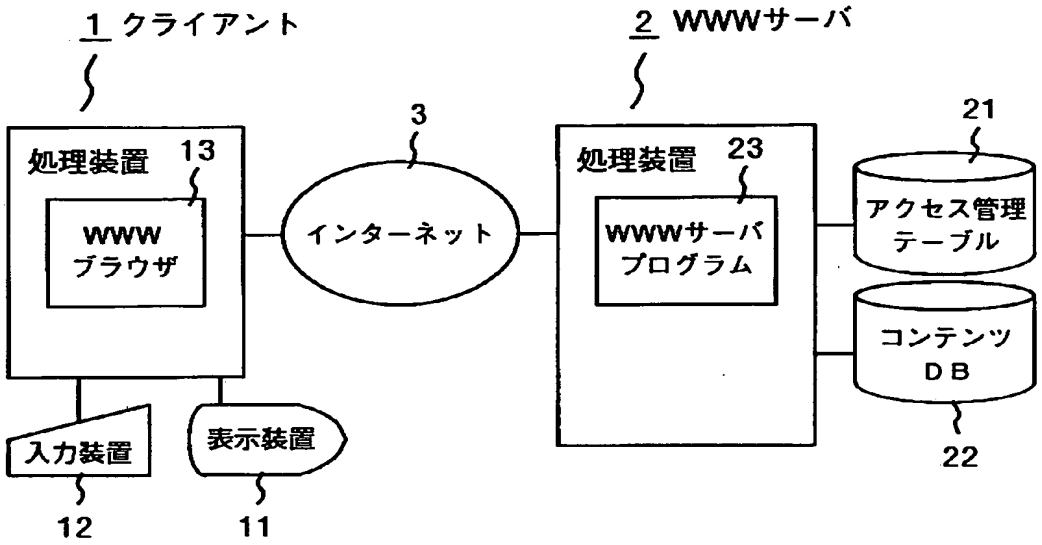
【符号の説明】

１：クライアント、２：ＷＷＷサーバ、３：インターネット、１３：ＷＷＷブラウザ、２１：アクセス管理テーブル、２２：コンテンツＤＢ、２３：ＷＷＷサーバプログラム、４１：アクセス番号、４２：公開鍵、４３：秘密鍵

【書類名】　図面

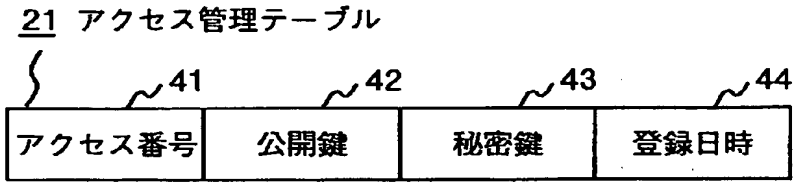
【図１】

図　1



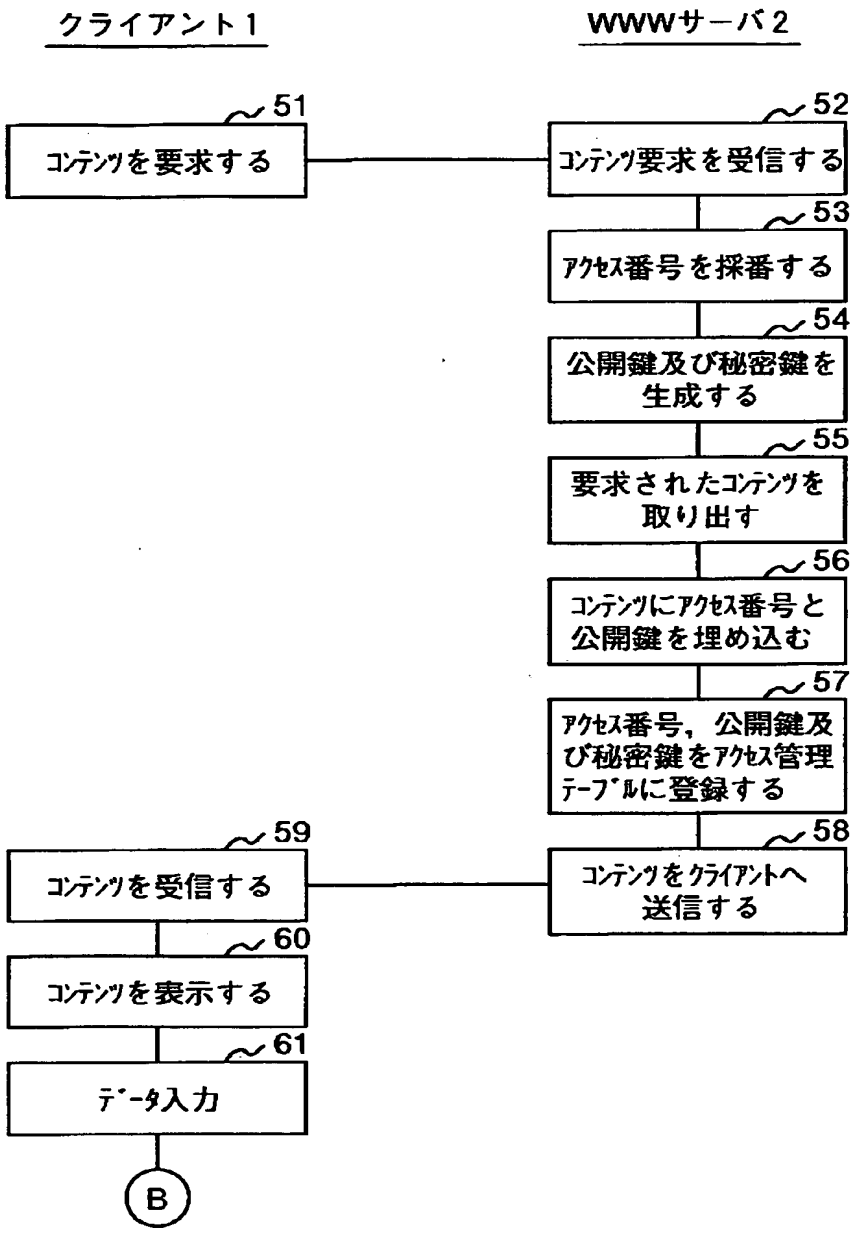
【図２】

図　2



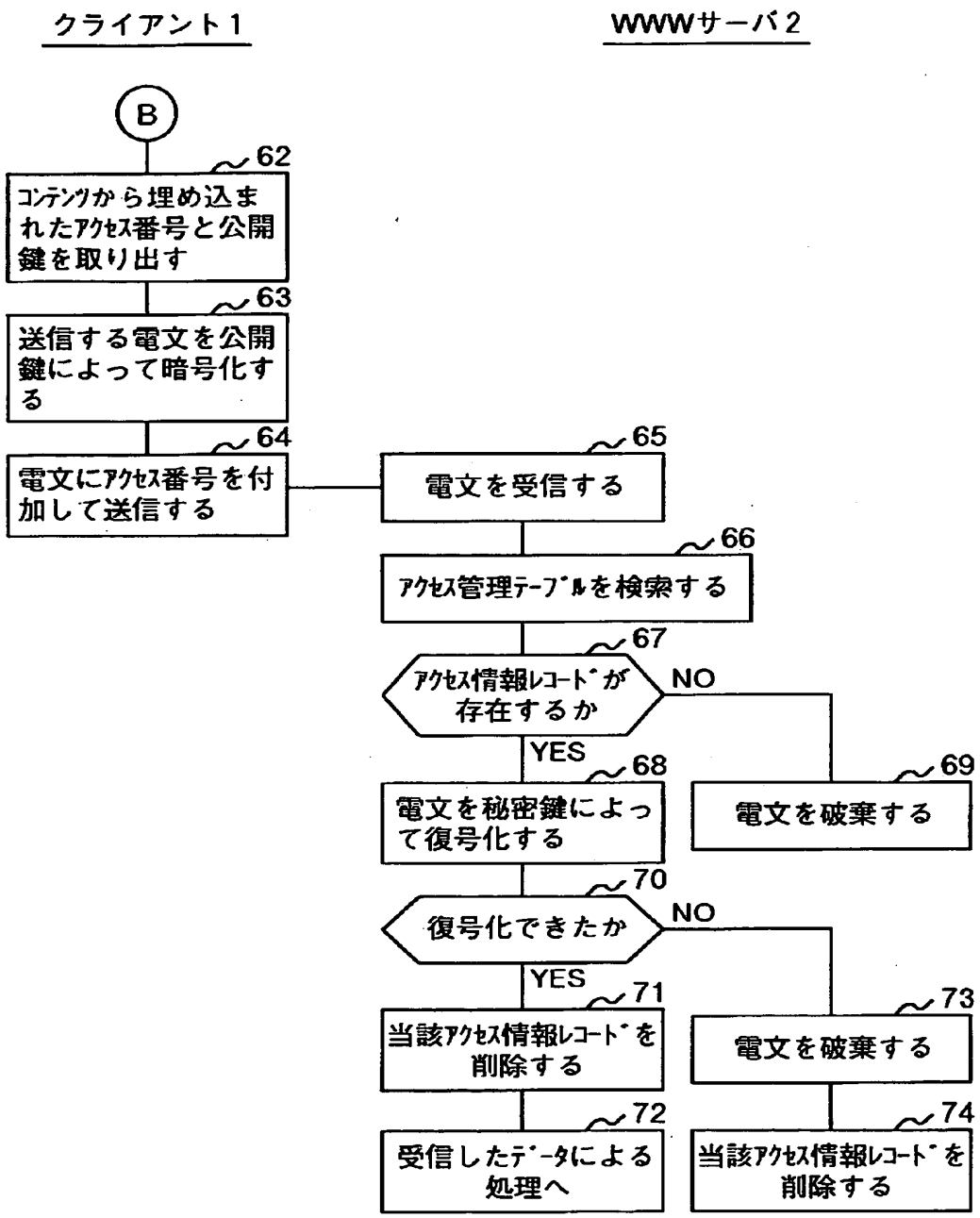
【図３Ａ】

図　３Ａ


クライアント1
WWWサーバ2
51
コンテンツを要求する
52
コンテンツ要求を受信する
53
アクセス番号を採番する
54
公開鍵及び秘密鍵を生成する
55
要求されたコンテンツを取り出す
56
コンテンツにアクセス番号と公開鍵を埋め込む
57
アクセス番号，公開鍵及び秘密鍵をアクセス管理テーブルに登録する
58
コンテンツをクライアントへ送信する
59
コンテンツを受信する
60
コンテンツを表示する
61
データ入力
B

【図３Ｂ】

図　３Ｂ


クライアント１
WWWサーバ２
B
62
ｺﾝﾃﾝﾂから埋め込まれたｱｸｾｽ番号と公開鍵を取り出す
63
送信する電文を公開鍵によって暗号化する
64
電文にｱｸｾｽ番号を付加して送信する
65
電文を受信する
66
ｱｸｾｽ管理ﾃｰﾌﾞﾙを検索する
67
ｱｸｾｽ情報ﾚｺｰﾄﾞが存在するか
NO
YES
68
電文を秘密鍵によって復号化する
69
電文を破棄する
70
復号化できたか
NO
YES
71
当該ｱｸｾｽ情報ﾚｺｰﾄﾞを削除する
73
電文を破棄する
72
受信したﾃﾞｰﾀによる処理へ
74
当該ｱｸｾｽ情報ﾚｺｰﾄﾞを削除する

【書類名】　要約書

【要約】

【課題】　サーバからクライアントへ要求されたコンテンツを送信し、クライアントからサーバへこのコンテンツに関する入力データを送信するシステムにおいて、応答データが正当なコンテンツアクセスに関するデータであることを認証する。

【解決手段】　WWWサーバプログラム２３は、コンテンツのアクセス対応にアクセス番号を生成してアクセス管理テーブル２１に登録するとともに、このコンテンツ内にそのアクセス番号を埋め込んでクライアント１へ送信する。WWWブラウザ１３は、このコンテンツを表示し、このコンテンツに関して入力されたデータにコンテンツから取り出したアクセス番号を付加してWWWサーバ２へ送信する。WWWサーバプログラム２３は、受信したアクセス番号が登録済であるときに受信したデータの正当性を認証するとともに、登録されたアクセス番号を無効にする。

【選択図】図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所